



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

Master's Thesis of International Studies

**Data Protection of Digital Trade
and Trade Agreements
Concentrating on EU's Legal Development**

**디지털 무역의 개인정보보호와 통상협정
: 유럽연합법 발전을 중심으로**

February 2018

**Graduate School of International Studies
Seoul National University
European Area Studies Major**

Lee, Hyesu

디지털 무역의
개인정보보호와 통상협정
- 유럽연합법 발전을 중심으로 -

지도 교수 안 덕 근

이 논문을 국제학석사 학위논문으로 제출함
2018년 2월

서울대학교 국제대학원
유럽지역학
이 혜 수

이혜수의 국제학석사 학위논문을 인준함
2018년 2월

위 원 장 _____ 문 우 식 (인)

부위원장 _____ 이 영 섭 (인)

위 원 _____ 안 덕 근 (인)

Data Protection of Digital Trade and Trade Agreements

Concentrating on EU's Legal Development

Ahn, Dukgeun

**Submitting a master's thesis of International Area Studies
February 2018**

**Graduate School of International Studies
Seoul National University
European Area Studies Major**

Lee, Hyesu

**Confirming the master's thesis written by
Lee, Hyesu
February 2018**

Committee Chair



Moon, Yoo-Sik

Committee Vice Chair



Rhee, Yeongseop

Thesis Advisor



Ahn, Dukgeun

Abstract

Data Protection of Digital Trade and Trade Agreements Concentrating on EU's Legal Development

Along with the development of digital technology, digital forms of trade volumes have been enlarged dramatically. These trades inevitably contain transactions of personal data which arouse concerns over possible misuses. However, trade regulations under the World Trade Organization (WTO) regime and other Free Trade Agreements cannot fully prevent privacy infringement and provide proper remedy measures for individuals.

This paper studies the long experiences and efforts of the European Union (EU) which has developed the legal foundations for protecting personal data while maintaining its free flow among countries. In particular, the study concentrates on how the efforts are reflected on the international agreements that the EU concluded and compares those agreements with other international trade regulations.

What was interesting was that all the regulations in typical trade agreements naturally linked the data protection concern to the human rights which had long been dismissed when dealing with trade concerns. Most of the trade agreements, however, are limited in providing appropriate remedy

measures for each individual in that these agreements are based on inter-governmental relationships and advocate collective interests of domestic industries.

Unlike other trade agreements, the Privacy Shield Principles, which was agreed between the EU and the U.S. following the nullification of previous Safe Harbor Agreement, is introduced as the most concrete and effective regulations for protecting personal data from companies that may infringe the agreement. As a legal area that does not have unified multilateral frame to regulate the digital trade concern, harmonizing the regulation would enhance market efficiency and predictability of participants. The EU-US Privacy Shield Principles that the two trade giants have already compromised can be model clauses for further harmonizing current fragmented international regulations.

Keyword: Digital Trade, Data Protection, EU-US Privacy Shield Principles, Remedy Measures, Harmonization of Law

Student Number: 2013-22071

Table of Contents

I. Introduction	1
II. Privacy Protection of European Union.....	4
1. Early Legal Development for Data Protection	
2. General Data Protection Regulation	
3. The Safe Harbor Agreement	
4. EU-US Privacy Shield Framework Principle	
III. Privacy Protection of International Trade Agreements	23
1. Regulation under the World Trade Organization	
2. Regulation under the Free Trade Agreements	
2.1. Regional Regulations on the Data Protection	
2.2. Bilateral Free Trade Agreements	
2.2.1. US-Korea Free Trade Agreement	
2.2.2. EU-Korea Free Trade Agreement	
2.2.3. The Comprehensive Economic and Trade Agreement	
2.2.4. The Transatlantic Trade and Investment Partnership	
2.3. Trans Pacific Partnership	
IV. Privacy Protection of Digital Trade	49
1. Special Natures of the Discussion	
2. Limits of Existing Regulations	
3. Harmonization of Data Protection Regulations in Trade Area	
V. Conclusion.....	59
Bibliography.....	61
Abstract in Korean	65

I. Introduction

1. Study Background

Free movement of data is an integral part of the digital trade. A transaction, at the same time, necessarily involves collections and uses of personal data, such as credit card number, ethnic origins, searching history, visited places, medical records and various private tastes, which can be used to identify or imply specific individuals online. Accordingly, a transaction requires strict regulations and broad consents among data traders in terms of its processing process.

Apart from the conservative attitude toward the digital trade of some countries including the Chinese government, the major norm-setting players, the European Union (EU) and the United States (U.S.), have agreed upon the importance of free movements and the protection of personal information at the same time. Nevertheless, their approaches to the issue are fundamentally different. While the U.S. allows collecting, and processing the personal data unless these activities cause any harm or conflict with the national law, the EU allows data transaction only if there is an explicit legal basis. European countries' experiences of the WWII when personal data was

abused as extracting specific ethnic derived comprehensive consents from the European citizens that the private information may threaten even the human rights and it should be dealt with high caution.

2. Research Purpose

Despite the astonishing enlargement of digital trade volume and its impacts on every country and individual, international trade regulations do not seem to fully reflect its development of today. The digital trade renders existing discussions and premises of GATT and WTO does not suffice to rule the current trade aspects. Previous discussions and understandings are mainly dealing with trade in goods produced based on comparative advantages derived from specific geological and historical features of certain environments. However, these general premises may be worthless in terms of the digital trade. Starting from the definition of the digital trade, deciding which chapter of the WTO should be applied to bind the non-participants of plurilateral trade agreements such as TiSA are still unclear concerning the digital trade issue.

More than 60 countries have tried to adopt data protection or privacy

laws to discipline the information flow on the Internet. Yet, these regulations are having different objectives, rationales, and legal reach. Consequentially, regulations are neither efficient nor consistent. Considering the nature of information that leaked information cannot be retrieved, adjusting and filling the gaps between the degrees of protection among different countries would be vital. Meanwhile, the EU is considered to have a well-developed data protection law which achieved significant consistency within its continent. Such leadership in data protection law has influenced far beyond its territory since the main principles of its law have been borrowed and reflected in numerous other countries' privacy laws.¹

Against this background, the main objective of this dissertation is to derive implications from the legal experiences of the EU when regulating privacy invasions in digital trade. This paper will examine the recent ongoing discussions within the European Union that strives to balance between the blooming digital trade, individual privacy concerns and international trade regulations including the World Trade Organization, Free Trade Agreements, and Trans Pacific Partnership. Among other things, studying remedy measures for online privacy protection is the main reason for applying EU's perspective to the international trade regulations.

¹ UNCTAD. 2016. *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. 32.

II. Privacy Protection of European Union

1. Early Legal Developments for Data Protection

The EU has been the leader in global efforts to advance online privacy protection. Public supports for strong data protection has a long and proud history in the Europe. Since all EU member states are also members of the Council of Europe, and thus they are required to secure the protection of personal data under human rights law. Every EU citizen has the right to keep his or her personal data privately protected and firms can only collect such data under specifically restricted conditions.²

The Council of Europe Data Protection Convention of 1981(Convention 108)³ was the earliest binding pledge for the data protection.⁴ The Convention is open to non-European countries and currently 51 member states, including all EU countries, have ratified the Convention⁵ and pledged to implement their own national laws which

² Susan Ariel Aaronson. 2016. *The Digital Trade Imbalance and Its Implications for Internet Governance*. CIGI. Chatham House. 12.

³ The official title of the Convention is ‘Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data’

⁴ Council of Europe Portal. “Convention 108 and Protocol” Accessed January 21. 2018. <https://www.coe.int/en/web/data-protection/convention108-and-protocol>.

⁵ Council of Europe Portal. “Details of Treaty No. 108”. Accessed January 21.

comply with the Convention.⁶ Article 7 of the Convention “requires appropriate security measures shall be taken for the protection of personal data stored in the automated data files.” Article 8 also provides additional safeguards measures whereby one can rectify and delete his or her personal data if the data have been used or treated unlawfully. Although the Convention did not provide further elaboration about the meanings of ‘appropriate security measures’, the Article 11, clearly states Extended Protection does not limit the scope of measures as it reads that “none of the provisions of the chapter *shall* be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention.”

The EU also requires member states to investigate privacy violations. The European Commission’s Directive on Data Protection went into effect in October 1998 and it prohibits the transfer of personal data to non-EU countries that do not meet the EU “adequacy” standard for privacy protection. The Article 25(6) gave the European Commission the authority to

2018. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/>.

⁶ Article 4 (Duties of the Parties)

1 Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2 These measures shall be taken at the latest at the time of entry into force of this Convention in respect of that Party.

determine the level of the “adequacy” and admitted 10 countries⁷ as having adequate protection degrees. The EU also requires other countries to create independent government data protection agencies, register databases with those agencies and, in some instances, obtain prior approval before the process begins. Meanwhile, to bridge these differences in regulatory strategy, the U.S. Department of Commerce in consultation with the European Commission developed a “Safe Harbor” framework.

⁷ Andorra (2010), Argentina (2003), Canada (2002), Switzerland (2004), Faeroe Islands (2010), Israel (2011), Isle of Man (2004), Jersey (2008), New Zealand (2013), Uruguay (2012).

2. General Data Protection Regulation

In 2016, the EU introduced General Data Protection Regulation (GDPR) in order to unify different regulations among member countries and to enhance binding force of data protection within the EU by empowering legal rights of EU citizens. The regulation was recognized in April 2016 and it will be enforced from May 2018 replacing the Directive on Data Protection. The preamble of the Directive emphasized that the protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the Charter) and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the rights to protect his or her personal data.

Unlike the Directive, members do not need to enact separate enabling legislation under the GDPR, thus it is automatically bound and applicable within the EU. It is also applicable to all companies processing personal data of EU citizen regardless of the company's geological location and, if breached, the fine can be as large as 4% of its annual turnover or 20 million euro. Data processing companies should ask for consents from owners in an easily understandable and accessible manner and provide legible terms.

3. The Safe Harbor Agreement

The Safe Harbor Agreement had allowed transmission of European citizen's digital data to the U.S. until its recent ruling of invalidation by the European Court of Justice (EUCJ) in 2000. The Agreement was designed to prevent accidental disclosure of personal data stored in the EU or the U.S. territory to other third countries. The European Commission approved the Safe Harbor framework as a special 'adequate' mechanism for US businesses. Under this agreement, certain US companies can voluntarily *self-certify* that they comply with the Safe Harbor Principles, and thereby can *be deemed* as adequate under the EU Directive.⁸ The Agreement reflected the Data Protection Directive (DPD) on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC) in 1995 followed by earlier non-binding recommendation of the OECD that personal data should be protected under the form of seven principles in 1980.⁹

The EUCJ, however, judged that the Agreement was not sufficient enough to ease its privacy concern of European citizen based on the Treaty

⁸ UNCTAD. 2016. *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. 33.

⁹ Notice, Purpose, Consent, Security, Disclosure, Access, and Accountability.

of Lisbon and the Charter of Fundamental Rights of the EU in 2015. The decision was evoked by an Austrian national, Maximillian Schrems, who expressed his worries over any accidental leakage of his personal data on Facebook in the U.S. while following the revelation of Edward Snowden about the extent of NSA eavesdropping. The Irish Data Protection Act (DPA),¹⁰ as the court of the first trial, dismissed the complaint, finding that it had no basis to evaluate the complaint since Facebook adhered to the Safe Harbor Agreement which was recognized as “adequate” by the European Commission. Upon request by the Irish High Court, the EUCJ examined whether the Irish DPA *could conduct* an investigation into Facebook’s data protection practices to assess their adequacy or the Irish DPA *had to defer* to the European Commission’s earlier approval of the Safe Harbor framework.

The EUCJ found that the “existence of Safe Harbor Agreement did not eliminate or reduce the power available to the national DPAs” and thus the DPA could investigate Facebook whether it complied with the DPD and the EU’s Charter of Fundamental Rights. Moreover, the EUCJ found that the “European Commission was required to examine domestic laws or international commitments of a third country prior to determining the

¹⁰ The Office of the Data Protection Commissioner is the independent national authority responsible for upholding the EU fundamental right of individuals to data privacy through the enforcement and monitoring of compliance with data protection legislation in Ireland.

adequacy of the country's data privacy protection according to Article 25 of the DPD." The Commission recognized that the Safe Harbor Agreement did not fulfill the requirements and thus the decision would not be valid any longer. As a result, US companies including Google, Facebook must introduce model contract clauses to be authorized for gathering personal data from the EU.

4. EU-US Privacy Shield Framework Principle

4.1. The Privacy Shield

The Safe Harbor Agreement has been replaced by the EU-US Privacy Shield after the ruling of EUCJ. In the overview part of the Shield the U.S. Department of Commerce acknowledges the difference in regulating mechanism of both parties and announced that the “Department of Commerce is issuing these Privacy Shield Principles, including the Supplemental Principles under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512).” It also emphasized that the “principles are intended to use solely by organizations in the U.S. receiving personal data from the EU for the purpose of qualifying for the Privacy Shield and thus benefitting from the European Commission’s adequacy decision.”

Following the framework regulation, the U.S. Department of Commerce will monitor its companies processing data from the Europe and both parties will review the implementation annually.¹¹ The European

¹¹ Annegret Bendiek and Evita Schmieg. 2016. *European Union Data Protection and External Trade*. German Institute for International and Security Affairs. 6.

Commission highlights several factors as distinctive features of the new arrangement; obligating stronger data protection policies for companies receiving personal data from the EU, introducing safeguard measures regarding the U.S. government's access to personal data, preparing effective protection and redress measures for individuals, and holding annual joint review for implementation.¹² Under the Attachment A, the U.S. also provided an overview of the U.S. privacy and security landscape as below:

“The protections provided by the EU-U.S. Privacy Shield Framework exist in the context of the broader privacy protections afforded under the U.S. legal system as a whole. First, the U.S. Federal Trade Commission has a robust privacy and data security program for U.S. commercial practices that protects consumers worldwide. Second, the landscape of consumer privacy and security protection in the United States has evolved substantially since 2000 when the original U.S.-EU Safe Harbor program was adopted. Since that time, many federal and state privacy and security laws have been enacted and public and private litigation to enforce privacy rights has increased significantly. The broad scope of U.S. legal protections for consumer privacy and security applicable to commercial data practices complements the protections provided to EU citizens by the new Framework.”

U.S. companies that want to receive personal data from the EU must

¹² European Commission. 2016. *Guide to the EU-US Privacy Shield*. 9-13.

sign up with the U.S. Department of Commerce and enact their own binding regulation in parallel with the Privacy Shield. Companies under obligations should inform the data providers of types and purposes of data to collect, rights to access to their own personal data and procedures of filing complaints concerning the data processing. In principle, the collected data cannot be used for purposes other than the originally consented ones. However, different yet related purposes can be allowed unless providers expressly object by 'opt-out' or the data is considered to be 'sensitive data' that requires further consent called 'opt-in'. Companies must also keep the personal data secured against unexpected loss, misuse, unauthorized access, disclosure, alteration or destruction, and should take due account on the nature of the data and the risks involved in processing.

In addition, companies' policy implementation should be reviewed annually. If its annual examination reveals that the company failed to comply with the Privacy Principle, it will be fined or removed from the list of companies which properly complies with the Privacy Shield. These results are published on the website of the Department of Commerce so that individual consumers can also find which companies are reliable enough to provide their individual information.

All data providing individuals have the rights to access and correct

their own personal data. Individuals have the right “to have their data communicated to themselves but also to get information about the purpose in which the data are processed in the categories of personal data concerned and the recipients to whom the data are disclosed.” A data processing company should respond to the request within a reasonable time. When personal information was used for making a decision against an individual’s interest, he or she can be provided with further explanation regarding which data were used and how the decision was made.¹³

4.2. Violation of the Privacy Shield

If companies failed to observe the Privacy Shield obligations, anyone can complain about the violation and get a remedy without any cost. The Agreement ensures remedies by obliging companies to provide such measures through independent recourse mechanism along with the U.S. Department of Commerce, U.S. Federal Trade Commission and Privacy Shield Panel.

One can express his or her complaints to the company itself first.

¹³ Ibid. 11.

Then independent recourse mechanisms such as Alternative Dispute Resolution or national Data Protection Authority would be the next options if the initial attempt fails. In case of the ADR, U.S. companies can choose between the U.S. and the EU ADR and the procedure also depends on the selected ADR body. Each EU member state also has its own Data Protection Authority responsible for protecting and enforcing the data protection rules at its national levels. Individuals can file complaints through the Department of Commerce and the U.S. Federal Commission in the U.S.

Supplemental principles on dispute resolution and enforcement are stipulated as below:

d. Recourse Mechanisms

i. “Consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Organizations must respond to a consumer within 45 days of receiving a complaint. Whether a recourse mechanism is independent is a factual question that can be demonstrated notably by impartiality, transparent composition and financing, and a proven track record. As required by the Recourse, Enforcement and Liability Principle, the recourse available to individuals must be readily available and free of charge to individuals. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of

eligibility requirements by the organization operating the recourse mechanism, but such requirements should be transparent and justified (for example, to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in conformity with the Privacy Shield Principles. They should also cooperate in the development of tools such as standard complaint forms to facilitate the complaint resolution process."

ii. *"Independent recourse mechanisms must include on their public websites information regarding the Privacy Shield Principles and the services that they provide under the Privacy Shield. This information must include: (1) information on or a link to the Privacy Shield Principles' requirements for independent recourse mechanisms; (2) a link to the Department's Privacy Shield website; (3) an explanation that their dispute resolution services under the Privacy Shield are free of charge to individuals; (4) a description of how a Privacy Shield-related complaint can be filed; (5) the timeframe in which Privacy Shield-related complaints are processed; and (6) a description of the range of potential remedies."*

If all these channels were found to be ineffective, one can rely on an arbitration mechanism known as a Privacy Shield Panel. The panel consists of three neutral arbitrators. Although this arbitration does not require a

presence in court, the final decision has binding power in the U.S.¹⁴

¹⁴ Article 7 (Recourse, Enforcement and Liability)

a. Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:

i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;

ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of noncompliance; and

iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints.

c. Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.

d. In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

e. When an organization becomes subject to an FTC or court order based on noncompliance, the organization shall make public any relevant Privacy Shield related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The Department has

Annex I, Arbitral Model of the Shield is designed to provide a prompt, independent, and fair mechanism for resolving claims which remain unsolved by any other Privacy Shield mechanisms. Firstly, the scope for applying the arbitration is as below:

A. Scope

“This arbitration option is available to an individual to determine, for residual claims, whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles or with respect to an allegation about the adequacy of the Privacy Shield.”

The arbitration on implementing obligations under the Privacy Shield is provided for each individual against organizations get personal data from the EU countries. The initiation of the arbitration procedure is laid under individuals’ own decision; however, the final decision of arbitration will have binding forces to each party. The agreed panel can impose “individual

established a dedicated point of contact for DPAs for any problems of compliance by Privacy Shield organizations. The FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

specific and non-monetary remedies such as access, correction, deletion, or return of the personal data in question” which are necessary to rectify the violation of the Principles. The relevant provision is as below:

B. Available Remedies

“Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual’s data in question) necessary to remedy the violation of the Principles only with respect to the individual. These are the only powers of the arbitration panel with respect to remedies. In considering remedies, the arbitration panel is required to consider other remedies that already have been imposed by other mechanisms under the Privacy Shield. No damages, costs, fees, or other remedies are available. Each party bears its own attorney’s fees.”

Close collaborations between European data protection authorities and its U.S. counterparts is the premise for these remedies. According to the Shield mechanism, the EU Commission is relying on permissions of the U.S. authorities for assuring court approach by the EU citizens in the U.S. territory. And the implementation of court’s decision can be judicially reviewed pursuant to the U.S. law under Federal Arbitration Act.

Despite these recourse measures, if an entity persistently refuses to

comply with the Principles, it will not be considered as a complying company of the Privacy Shield principle. The organization will be removed from the list by the Department within 30 days of notice and it must return or delete the personal information they have.¹⁵

Moreover, the Privacy Shield has an independent ombudsperson mechanism as its unique remedy method when it deals with national security issue. EU citizens who believe their personal data were misused due to the U.S. national security reasons can bring the case to the ombudsperson. The ombudsperson is a secretary of the State designated as a senior coordinator for international information technology diplomacy who serves as a point of contact for EU citizens. The Annex A of the Privacy Shield stipulates this mechanism and it starts with a quoted speech of former U.S. President Obama delivered on January 17, 2014. He said “Our efforts to protect personal data not only help the State, but its friends and allies as well. Our efforts will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy too.”

The U.S. businesses also largely depend on the data security for their

¹⁵ Article 11.g (Persistent Failure to Comply)

i. If an organization persistently fails to comply with the Principles, it is no longer entitled to benefit from the Privacy Shield. Organizations that have persistently failed to comply with the Principles will be removed from the Privacy Shield List by the Department and must return or delete the personal information they received under the Privacy Shield.

intellectual property protection while seeking maximization of data free flow respectively. Thus, the ombudsperson is required to properly investigate and address complaints in a timely manner. Throughout this procedure, the ombudsperson will work closely but independently with appropriate officials from other departments and agencies who are responsible for processing requests in accordance with applicable U.S. laws and policies.¹⁶ As receiving investigation requests, the EU individual complaint handling body will first verify the identification of the individual and ensure that the person is acting on his or her own behalf not as a representative of a governmental or intergovernmental organization. After confirming several terms of submission, the ombudsperson can precede investigations and recommend corrective actions regarding violation.

¹⁶ ANNEX A (EU-U.S. Privacy Shield Ombudsperson Mechanism) Article 2.a.

III. Privacy Protection of International Trade Agreements

1. Regulation under the World Trade Organization

As a long-standing criterion of international trade regime, the World Trade Organization (WTO) has been served as the most important and binding trade agreement since 1995. Under the WTO regime, the General Agreement on Tariffs and Trade (GATT) rules on trade in goods including digital products and the General Agreement on Trade in Service (GATS) is dealing with the digital service trade in a most general way as a cross-border information service.

The WTO adopted the ‘Work Program on Electronic Commerce’ and defined the electronic commerce as ‘the production, distribution, marketing, sale or delivery of goods and services by electronic means in 1998.’¹⁷ Nevertheless, there remains unclear area when defining the meaning of digital contents. The Appellate Body (AB) of China-Publications and Audiovisual Products (DS363) recognized its complexity when it comes to judge which chapter of the WTO should be applied in dealing with digital contents trade issue. The AB said, “Even if cinematographic films are

¹⁷ WTO. Electronic Commerce. Accessed December 10. 2017.
https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm

imported simultaneously, physically in conjunction with the right to provide the service in question, this does not imply that the effects of the *Film Regulation* on goods, and on the importers of those goods, are somehow removed from the scope of applicability of China's trading rights commitments.”¹⁸ The AB found that importation of a film can be regulated by the GATT provisions as it has physical form of trade. At the same time, it can also be considered as the AB left arguable margin for application of the GATS by emphasizing *the physical form* of films. Thus, the AB did not exclude the possibility of applying GATS rules on digital contents without having the physical form.

Considering the fact that data protection issue is mostly arouse from non-physical form of trades and the GATT has no provision regarding data protection, the GATS would be a more proper subject to this discussion. Meanwhile, the GATS stipulates that the data protection is not an illegitimate barrier to competition under the Article XIV (General Exceptions) which applies to secure compliance with laws or regulations concerning the protection of the privacy of individuals. The Article XIV(c) (ii) is as below:

¹⁸ WTO. *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*. Report of the Appellate Body. 87-88.

“Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:

... (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:

... (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; ...”

However, these provisions of general exceptions are difficult to be applied as there are several requirements to be satisfied. Assuming a member country decided not to allow personal information to be provided to service providing companies in other territory based on the general exception clause, it would be difficult to be admitted as a reasonable exception. Even though members can take measures as arguing misused personal information threaten its public morals or compliance with laws or regulations, the panel and AB members judge the arguments according to two tier analyses. First, the protecting measure should be proven to be necessary to secure compliance with laws or regulations. The AB members of the U.S.-Measures Affecting the Cross-Border Supply of Gambling and Betting Service replaced the direct judgment with the judgment of Article

XIV(a) saying that “...the United State failed to explore and exhaust all reasonably available alternative measures.”¹⁹ Likewise, the necessity requires no other alternative measure to be found under the WTO regulation. Second, the Chapeau of the Article XVI would be the next condition to be satisfied. The Chapeau stipulates that “...measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in service...” In other words, the GATS has uncertain languages regarding when member countries can constraint its services against other members and needs further arguments.

Meanwhile, the WTO has its unique dispute settlement mechanism called the Dispute Settlement Understanding (DSU) which provides the means for member countries to resolve conflicts. The Article 3 of DSU under Annex 2 prescribes that the “Members recognize that the DSU serves to preserve the rights and obligations of Members under the covered agreements, and to clarify the existing provisions of those agreements in accordance with customary rules of interpretation of public international law. Recommendations and rulings of the DSB cannot add to or diminish the rights and obligations provided in the covered agreements.” More than 500

¹⁹ WTO. *The U.S.-Measures Affecting the Cross-Border Supply of Gambling and Betting Service* (WT/DS285/AB/R). Report of the Appellate Body. 111.

disputes have been brought to the WTO and over 350 rulings have been issued since 1995.²⁰ The dispute settlement procedure largely has three stages: (1) consultations; (2) panel and, if requested, appellate body review; and (3) if needed, implementation.²¹

Member states should attempt to solve its problems through consultations, ahead of any other means according to the Article 4.²² If the consultation fails, the complaining party could request to the panel for further examination. Once the request is submitted to the DSB as an agenda, the panel shall be established at the following DSB meeting, unless the DSB decides by consensus not to establish a panel.²³ The panel procedures for

²⁰ WTO. “Dispute Settlement”. Accessed December 22, 2017. https://www.wto.org/english/tratop_e/dispu_e/dispu_e.htm.

²¹ Daniel T. Shedd, Brandon J. Murrill, and Jane M. Smith. *Dispute Settlement in the World Trade Organization: An Overview*. Congressional Research Service. 4.

²² Article 4 (Consultations)

2. Each Member undertakes to accord sympathetic consideration to and afford adequate opportunity for consultation regarding any representations made by another Member concerning measures affecting the operation of any covered agreement taken within the territory of the former.

3. If a request for consultations is made pursuant to a covered agreement, the Member to which the request is made shall, unless otherwise mutually agreed, reply to the request within 10 days after the date of its receipt and shall enter into consultations in good faith within a period of no more than 30 days after the date of receipt of the request, with a view to reaching a mutually satisfactory solution. If the Member does not respond within 10 days after the date of receipt of the request, or does not enter into consultations within a period of no more than 30 days, or a period otherwise mutually agreed, after the date of receipt of the request, then the Member that requested the holding of consultations may proceed directly to request the establishment of a panel.

²³ Article 6 (Establishment of Panels)

panel formation are specifically requires well-qualified composition,²⁴ objective assessment,²⁵ and confidentiality of panel deliberation²⁶ until the adoption period²⁷ in order to assure a fair and effective panel review.

1. If the complaining party so requests, a panel shall be established at the latest at the DSB meeting following that at which the request first appears as an item on the DSB's agenda, unless at that meeting the DSB decides by consensus not to establish a panel.

2. The request for the establishment of a panel shall be made in writing. It shall indicate whether consultations were held, identify the specific measures at issue and provide a brief summary of the legal basis of the complaint sufficient to present the problem clearly. In case the applicant requests the establishment of a panel with other than standard terms of reference, the written request shall include the proposed text of special terms of reference.

²⁴ Article 8 (Composition of Panels)

1. Panels shall be composed of well-qualified governmental and/or non-governmental individuals, including persons who have served on or presented a case to a panel, served as a representative of a Member or of a contracting party to GATT 1947 or as a representative to the Council or Committee of any covered agreement or its predecessor agreement, or in the Secretariat, taught or published on international trade law or policy, or served as a senior trade policy official of a Member.

²⁵ Article 11 (Function of Panels)

The function of panels is to assist the DSB in discharging its responsibilities under this Understanding and the covered agreements. Accordingly, a panel should make an objective assessment of the matter before it, including an objective assessment of the facts of the case and the applicability of and conformity with the relevant covered agreements, and make such other findings as will assist the DSB in making the recommendations or in giving the rulings provided for in the covered agreements. Panels should consult regularly with the parties to the dispute and give them adequate opportunity to develop a mutually satisfactory solution.

²⁶ Article 14 (Confidentiality)

1. Panel deliberations shall be confidential.

2. The reports of panels shall be drafted without the presence of the parties to the dispute in the light of the information provided and the statements made.

3. Opinions expressed in the panel report by individual panelists shall be anonymous.

²⁷ Article 16 (Adoption of Panel Reports)

1. In order to provide sufficient time for the Members to consider panel reports, the reports shall not be considered for adoption by the DSB until 20 days

Unlike any other international dispute settlement body, the DSU also has an appellate review procedure as an appealing trial. Article 17.6 of the DSU limits its appeals to issues of law covered in the panel report and legal interpretations developed by the panel. Within 60 days of being notified from an appeal (extendable to 90 days), the Appellate Body (AB) must issue a report that upholds, reverses, or modifies the panel report. The AB report is to be adopted by the DSB, and unconditionally accepted by the disputing parties, unless the DSB decides by consensus not to adopt it within 30 days after the report is shared by the members.²⁸

after the date they have been circulated to the Members.

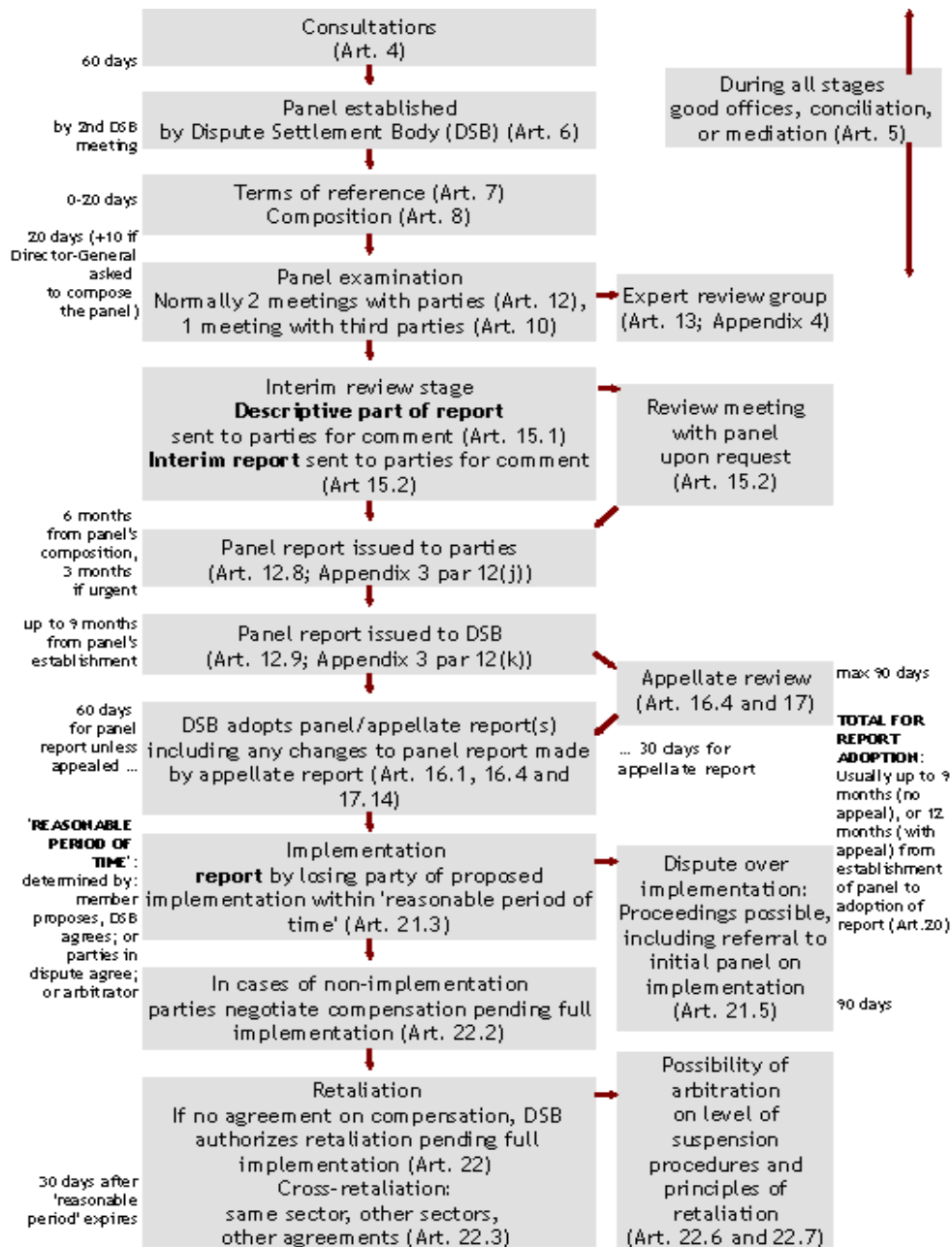
2. Members having objections to a panel report shall give written reasons to explain their objections for circulation at least 10 days prior to the DSB meeting at which the panel report will be considered.

3. The parties to a dispute shall have the right to participate fully in the consideration of the panel report by the DSB, and their views shall be fully recorded.

4. Within 60 days after the date of circulation of a panel report to the Members, the report shall be adopted at a DSB meeting⁷ unless a party to the dispute formally notifies the DSB of its decision to appeal or the DSB decides by consensus not to adopt the report. If a party has notified its decision to appeal, the report by the panel shall not be considered for adoption by the DSB until after completion of the appeal. This adoption procedure is without prejudice to the right of Members to express their views on a panel report.

²⁸ Daniel T. Shedd, Brandon J. Murrill, and Jane M. Smith. *Dispute Settlement in the World Trade Organization: An Overview*. Congressional Research Service. 7.

[Flow Chart of the Dispute Settlement Process] ²⁹



²⁹ WTO. "The Process". Accessed December 22, 2017.

https://www.wto.org/english/tratop_e/dispu_e/dispu_settlement_cbt_e/c6s1p1_e.htm.

Apart from the GATT and GATS which are binding all participants as a single undertaking, the Trade in Service Agreement (TiSA) imposes obligations on only like-minded 23 WTO members³⁰ as an issue based plurilateral agreement. The negotiation firstly proposed in 2012 by the 'Really Good Friends' countries around the world led by the U.S. and the EU while the Doha Development Round had stayed in a long stalemate situation. The official negotiation began in 2013 with WTO member countries representing 70 percent of global services trade. The Agreement was built up on the GATS and thus every provision of the TiSA is compatible with the GATS. It aims to upgrade the previous GATS provisions for further liberalizing the service trade. The EU said the TiSA members expect its negotiation to be reflected on the WTO provisions hopefully by embracing other non-participants of the TiSA. The following image shows the plurilateral service agreement progressing into the existing GATS. The EU expects the GATS would be enhanced by the results of the plurilateral agreement. The EU thought that partial consensus within the WTO could be transformed into an annex to the GATS or each sectoral chapter could be turned into either understanding or reference papers under

³⁰ Australia, Canada, Chile, Chinese Taipei, Colombia, Costa Rica, the EU, Hong Kong China, Iceland, Israel, Japan, Korea, Liechtenstein, Mauritius, Mexico, New Zealand, Norway, Pakistan, Panama, Peru, Switzerland, Turkey, the United States.

the GATS article XVIII.³¹

Concerning the data protection issue, the EU publicized its fact sheet on the website of European Commission stating that the TiSA will contain the same safeguards for protecting data privacy as in the current GATS terms. It means that countries can continuously maintain their own confidentiality and data protection laws.³² EU proposal for an annex on financial service document also contains provision concerning the information transfer and personal data protection.³³ Meanwhile, it gives more weight on the personal data protection as it emphasized that “Nothing in this paragraph restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of this Agreement.” Although finalized legal text is not yet available, the EU added an explanation that the proposed document reflects the two existing

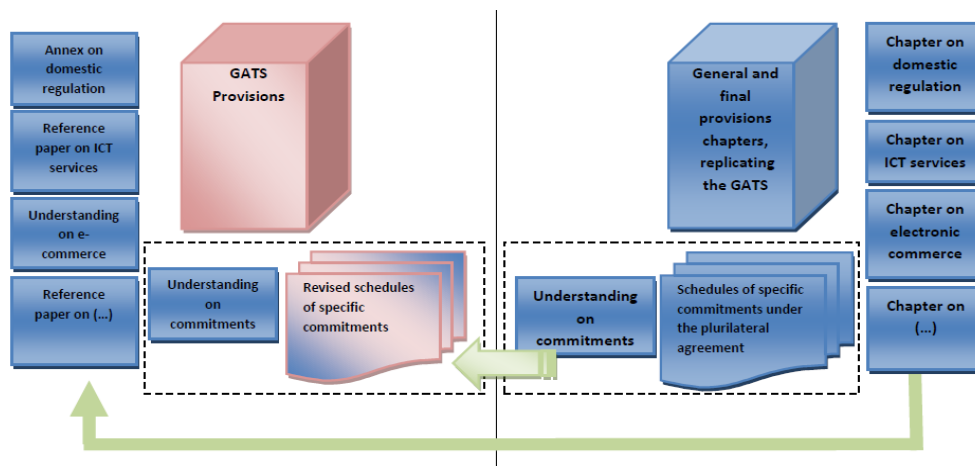
³¹ The European Union. 2012. *A modular approach to the architecture of a plurilateral agreement on service*. 5-6.

³² European Commission. 2016. *Trade in Service Agreement Fact Sheet*. 9.

³³ Article 14 (Transfers of Information and Processing of Information)

No Party shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier. Nothing in this paragraph restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of this Agreement.

agreements; the GATS annex on financial services and the GATS understanding on commitments in financial services. Judging from the explanation, current negotiations on the TiSA have not been preceded far beyond the existing WTO frame.



[Multilateralization of the Plurilateral Agreement]³⁴

³⁴ The European Union. 2012. *A modular approach to the architecture of a plurilateral agreement on services*. 6.

2. Regulations under Free Trade Agreements

2.1 Regional Regulations on Data Protection

The WTO regime aims to enlarge and sustain multilateral negotiation arena by imposing Article I GATT, ‘Most Favored Nation’ and Article III, ‘National Treatment’ principles as essential obligations to participating members. The WTO forum was founded on the shared understanding on how dangerous the mercantilist approach is.

However, it is hard to conclude a multilateral negotiation under the WTO due to its majority based on the decision-making system in which every member state exercises only one vote each. In addition, the single undertaking negotiation mechanism introduced during the Uruguay Round contributed as connecting links for segmented codes regulations but at the same time became a major reason for deadlock of the Doha Development Round.

The EU and the U.S. also faced the difficulties when they suggested not hindering the Internet service providers or the free flow of information online during the Doha Round negotiations in 2011. Although they wanted other member states to utilize multilateral regime to discuss about

information flows, cyber security and privacy protection, other participants did not respond to their proposal ardently as much as expected. Thus, the two players chose to deal with this issue through bilateral or regional trade agreements such as Free Trade Agreement, Transatlantic Trade and Investment Partnership, Trans Pacific Partnership.³⁵

³⁵ Susan Ariel Aaronson. 2016. *The Digital Trade Imbalance and Its Implications for Internet Governance*. CIGI. Chatham House. 8.

2.2. Bilateral Free Trade Agreements

2.2.1 US-Korea Free Trade Agreement

The U.S. and the Republic of Korea set rules regarding the free flow of information in the Electronic Commerce chapter under the frame of FTA for the first time in 2012. Article 15.8 of the agreement says that the “Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders”³⁶in general. Although no further elaboration was made to define the meaning of unnecessary barriers, one can infer that there can be exceptions for protecting private information as the Article considers not only the importance of the free flow of information but importance of protecting personal information.

Despite its progressed recognition, Aaronson and Towners assessed that the Article failed to include actionable languages. They argued that “Article 15.8 of the agreement says that the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information

³⁶ Article 15.8: Cross-Border Information Flows

Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.

flows across borders. However, this provision does not forbid the U.S. to employ such barriers, nor does it define what the necessary or unnecessary barriers are. Hence the reader does not know if legitimate exceptions to free flow of information, such as cyber-security measures or privacy regulations are necessary or not. It is unclear if one party could use this language to challenge another party's use of such barriers. Moreover, a party could always justify using such barriers under WTO exceptions to protect national security (the Chinese argument) or to protect public morals (the Russian argument).”³⁷

2.2.2 EU-Korea Free Trade Agreement

EU-Korea FTA also acknowledged the significance of both information transaction for digital trade and protection of personal information for protecting fundamental rights and freedom of individuals under Article 7.43 of the Trade in Service, Establishment and Electronic Commerce chapter.³⁸ The agreement mentioned that each Party shall adopt

³⁷ Aaronson, Susan A., M. Townes. 2012. *Can Trade Policy Set Information Free: Trade Agreements, Internet Governance and Internet Freedom*. Policy Brief. 6.

³⁸ ARTICLE 7.43: DATA PROCESSING

to adequate safeguards, however, nothing is further elaborated about the meaning of ‘adequate’ and how to deal with possible violations just as the KORUS FTA. Aaronson also assessed the EU-Korea FTA as having only aspirational language regarding the privacy.³⁹

2.2.3 The Comprehensive Economic and Trade Agreement

The Comprehensive Economic and Trade Agreement (CETA) is a free-trade agreement between the EU and Canada which was signed in October 2016. The negotiations for the CETA began in 2009 and were concluded in August 2014. Similar with the EU, Canada protects privacy as a fundamental right and the Canadian government explains that their priority was on protecting personal and commercial confidential information

No later than two years after the entry into force of this Agreement, and in no case later than the effective date of similar commitments stemming from other economic integration agreements:

(a) each Party shall permit a financial service supplier of the other Party established in its territory to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier; and

(b) each Party, reaffirming its commitment to protect fundamental rights and freedom of individuals, shall adopt adequate safeguards to the protection of privacy, in particular with regard to the transfer of personal data.

³⁹ Susan Ariel Aaronson. 2016. *The Digital Trade Imbalance and Its Implications for Internet Governance*. CIGI. Chatham House.13.

when consulting on the Agreement.⁴⁰

Under the chapter sixteen, electronic commerce, both parties agreed upon the importance of developing digital service industry⁴¹ and not imposing custom duties on the electronic deliveries except for the internal tax or other internal charges.⁴² In Article 16.4, they also mentioned about the trust and confidence in electronic commerce which are based on international standards of international organizations where both parties are members.

Distinguishing parts were the Article 16.6 and 16.7 which deal with dialogue on electronic commerce and the potential conflicts between the chapters, respectively. In the article 16.7 both parties emphasized

⁴⁰ Government of Canada. “CETA and Data Privacy”. Accessed November 27, 2017.http://boykoborissov.bg/sites/default/files/pictures/ceta_and_data_privacy.pdf.

⁴¹ Article 16.2 (Objective and scope)

1. The Parties recognise that electronic commerce increases economic growth and trade opportunities in many sectors and confirm the applicability of the WTO rules to electronic commerce. They agree to promote the development of electronic commerce between them, in particular by cooperating on the issues raised by electronic commerce under the provisions of this Chapter.

2. This Chapter does not impose an obligation on a Party to allow a delivery transmitted by electronic means except in accordance with the Party’s obligations under another provision of this Agreement.

⁴² Article 16.3 (Customs duties on electronic deliveries)

1. A Party shall not impose a customs duty, fee, or charge on a delivery transmitted by electronic means.

2. For greater certainty, paragraph 1 does not prevent a Party from imposing an internal tax or other internal charge on a delivery transmitted by electronic means, provided that the tax or charge is imposed in a manner consistent with this Agreement.

maintaining dialogue on the issue by exchanging information and experiences on their own regulations. In addition, Article 16.7 stipulates that other chapters of the CETA are dominant over the chapter 16, if there occurs any discrepancy issue between chapters.⁴³ These articles reveal that member countries are approaching this issue in a highly prudent manner and are not willing to take broad steps apart from the internationally accepted rules.

Meanwhile, the chapter on exceptions provides safeguard measures when adopting or enforcing a measure *necessary* to protect the privacy of individuals in relation to processing and disseminating data and to confidentiality of personal records and accounts.⁴⁴ The chapter on financial service supports the EU and Canada's enforcement of privacy legislation governing the cross-border transfer of personal information.⁴⁵ Article

⁴³ Article 16.7 (Relation to other Chapters)

In the event of an inconsistency between this Chapter and another chapter of this Agreement, the other chapter prevails to the extent of the inconsistency.

⁴⁴ Article 28.3 (General exceptions)

(c) to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts

⁴⁵ Article 13.15 (Transfer and processing of information)

2. Each Party shall maintain adequate safeguards to protect privacy, in particular with regard to the transfer of personal information. If the transfer of financial information involves personal information, such transfers shall be in accordance with the legislation governing the protection of personal information of

15.3(4) also requires parties to take *appropriate* measures to protect the privacy of public telecommunications transport service⁴⁶ and Article 16.4 necessitates both parties taking *international standard* for data protection of e-commerce users into consideration.⁴⁷ However, again, these languages do not seemingly imply further steps when it is compared to other international development of legislation on privacy protection issue. There remains controversy over concrete meanings of the necessary or appropriate measure. Enforcing legislation and considering international standard demand for another legal achievement as precedent condition.

2.2.4 The Transatlantic Trade and Investment Partnership

the territory of the Party where the transfer has originated.

⁴⁶ Article 15.3 (Access to and use of public telecommunications transport networks or services)

4. Further to Article 28.3 (General exceptions), and notwithstanding paragraph 3, a Party shall take appropriate measures to protect: (a) the security and confidentiality of public telecommunications transport services; and (b) the privacy of users of public telecommunications transport services, subject to the requirement that these measures are not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.

⁴⁷ Article 16.4 (Trust and confidence in electronic commerce)

Each Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce and, when doing so, shall take into due consideration international standards of data protection of relevant international organisations of which both Parties are a member.

Transatlantic Trade and Investment Partnership (TTIP) is an ongoing trade agreement between the EU and the U.S. Although its negotiation is temporally halted after the inauguration of President Donald Trump, it is still worth of notice since the TTIP is the largest bilateral trade initiative by the two largest economies in the world and its regulation would be a guide to later trade agreements.

While U.S. large multinational corporations tried to include the data protection issue under the TTIP discussions, the European Parliament is standing against it by as emphasizing that the personal data should remain under control of its individuals. Concerning the controversy, a digital law expert mentioned that “Data protection and privacy are fundamental human rights in Europe, while data is a monetized commodity in the U.S. Thus, for the American, the data protection and privacy are seen as impediments to free speech.” Another expert also pointed out this issue that “The EU Commission is negotiating TTIP on behalf of the EU and their obligation does not include a right to discuss or negotiate any fundamental rights.”⁴⁸

According to a leaked draft of the agreement, chapter VI is dealing with the electronic commerce issue. Article 62 of the chapter explains about the objective and principles in which both parties recognize the electronic

⁴⁸ John Leonard. 2016. *TTIP vs GDPR – who will win the data protection wars?* Computing Research. 6.

commerce increases trade opportunities and it shall be considered as cross-border supply of service without custom duties.⁴⁹ Besides, Article 63 mentioned that service providers have liability in respect to the transmission or storage of information and consumer protection in the ambit of electronic commerce.⁵⁰ Despite these shared understandings on the importance of data protection, the TTIP does neither specifically mention about the personal data protection method nor the term itself. Through its official factsheet released, the EU authority clarified that the “data protection standards won’t be part of TTIP negotiations and the EU’s data protection laws prevail over any commitments.” And the EC Trade Commissioner Karel de Gucht said

⁴⁹Article 62 (Objective and Principles)

1. The Parties, recognizing that electronic commerce increases trade opportunities in many sectors, agree to promote the development of electronic commerce between them, in particular by co-operating on the issues raised by electronic commerce under the provisions of this Title.

2. The Parties agree that electronic transmissions shall be considered as the provision of services, within the meaning of Chapter III (cross-border supply of services), which cannot be subject to customs duties.

⁵⁰ Article 63 (Regulatory aspects of e-commerce)

1. The parties shall maintain a dialogue on regulatory issues raised by electronic commerce, which shall inter alia address the following issues: the recognition of certificates of electronic signatures issued to the public and the facilitation of cross-border certification services, the liability of intermediary service providers with respect to the transmission, or storage of information, the treatment of unsolicited electronic commercial communications, the protection of consumers in the ambit of electronic commerce, any other issue relevant for the development of electronic commerce.

2. Such cooperation can take the form of exchange of information on the Parties’ respective legislation on these issues as well as on the implementation of such legislation.

that the “data protection is outside the scope of TTIP.”⁵¹ Besides, the EU is known to have suggested stronger personal data protection standard to the U.S., while, at the negotiation table of the WTO TiSA, the U.S. proposed to adopt general regulation on all service areas to allow cross-border data transfer including personal information.⁵²

⁵¹ Vivian Reding. 17 September 2013. *Data Protection Reform: Restoring Trust and Building the Digital Single Market*. Speech Delivered at the 4th Annual European Data Protection & Privacy Conference Brussels. 3.

⁵² KIEP. 2015. 국제 디지털 상거래의 주요 쟁점과 한국의 대응방안. 97.

2.3. Trans Pacific Partnership (TPP)

The U.S. went one step further after the KORUS FTA by including more actionable languages in the Trans Pacific Partnership (TPP) referring to languages of the KORUS FTA. Based on American initiative, Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam were 12 participants of the agreement originally signed on 4 February 2016. However, it is currently being renegotiated by other 11 countries after the Trump Administration advocated that the free trade rendered its caused for Americans in losing their jobs.

Despite the sudden withdrawal, its expected importance in the international trade arena still remains great. Susan Ariel Aaronson assessed that “The TPP is the first trade agreement to include binding commitments on cross-border information flows and to limit digital protectionism. Moreover, the agreement contains transparency requirements that could bring much-needed openness, due process and increased political participation to trade (and Internet-related) policy making in countries such as Vietnam.”⁵³

The TPP Article 14.1 starts by defining the concepts of ‘digital

⁵³ Susan Ariel Aaronson. 2016. *The Digital Trade Imbalance and Its Implications for Internet Governance*. CIGI. Chatham House. 9.

product’, ‘electronic authentication’, ‘electronic transmission or transmitted electronically’, and ‘personal information’, respectively. The Article left rooms for discussion as it states that the “definition of digital product should not be understood to reflect a Party’s view on whether trade in digital products through electronic transmission should be categorized as trade in services or trade in goods.” Article 14.3 clearly emphasizes that aside from internal taxes or charges allowed under the TPP Agreement members cannot impose custom duties on electronic transmissions.⁵⁴ And the Article 14.4 states the non-discriminatory obligation.⁵⁵ It further highlights the less favorable treatment will not be apply to subsidies, grants, and broadcasting.

⁵⁴ Article 14.3: Customs Duties

1. No Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of one Party and a person of another Party.
2. For greater certainty, paragraph 1 shall not preclude a Party from imposing internal taxes, fees or other charges on content transmitted electronically, provided that such taxes, fees or charges are imposed in a manner consistent with this Agreement.

⁵⁵ Article 14.4: Non-Discriminatory Treatment of Digital Products

1. No Party shall accord less favourable treatment to digital products created, produced, published, contracted for, commissioned or first made available on commercial terms in the territory of another Party, or to digital products of which the author, performer, producer, developer or owner is a person of another Party, than it accords to other like digital products.⁴
2. Paragraph 1 shall not apply to the extent of any inconsistency with the rights and obligations in Chapter 18 (Intellectual Property).
3. The Parties understand that this Article does not apply to subsidies or grants provided by a Party, including government-supported loans, guarantees and insurance.
4. This Article shall not apply to broadcasting.

And the Article 14.13 prohibits localization except for achieving a legitimate public policy objective.⁵⁶

At the same time, Article 14.7, Online Consumer Protection, directly stipulates the provision for consumer protection in electronic commerce. It also mandates member countries adopt or maintain consumer protection laws at its national level. Cooperation among respective national consumer protection agencies is laid down in the provision for enhancing consumer welfare.⁵⁷

⁵⁶ Article 14.13: Location of Computing Facilities

1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.

2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

⁵⁷ Article 14.7 (Online Consumer Protection)

1. The Parties recognise the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent and deceptive commercial activities as referred to in Article 16.6.2 (Consumer Protection) when they engage in electronic commerce.

2. Each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.

3. The Parties recognise the importance of cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border electronic commerce in order to enhance

Article 14.8, Personal Information Protection repeatedly acknowledges the importance of consumer confidence in electronic commerce by requesting each party *shall* adopt or maintain a legal framework for personal information protection in a non-discriminatory manner.⁵⁸ The Article also mentions that the parties *should* provide information regarding the personal information protections such as how individuals can pursue remedies or how businesses can comply with any

consumer welfare. To this end, the Parties affirm that the cooperation sought under Article 16.6.5 and Article 16.6.6 (Consumer Protection) includes cooperation with respect to online commercial activities.

⁵⁸ Article 14.8: Personal Information Protection

1. The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce.
2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies.
3. Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction.
4. Each Party should publish information on the personal information protections it provides to users of electronic commerce, including how:
 - (a) individuals can pursue remedies; and
 - (b) business can comply with any legal requirements.
5. Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them.

legal requirements. Moreover, it does not forget to mention that each party should encourage the development of mechanisms to promote compatibility among different regulatory frame works. The consumer protection is not just declarative words but substantial words that can impose each party to enact or amend its domestic rules under the TPP regulation. In general, languages of the TPP clearly stipulate obligations for balancing between the free flow of data and the protection of personal data.

IV. Personal Data Protection in Digital Trades

1. Special Natures of the Discussion

The concern over the protection of personal data accompanied by digital trade is situated in the interim area of trade and human rights issues. Previous discussions on human right issues in trade were usually by-products of production procedures, such as child labor or labor exploitation. However, the human right issues related to personal data protection in the realm of digital trade are directly involved in the trade activity itself which cannot be discussed separately. Accordingly, there are several distinguishing characteristics of the legal developments concerning this issue.

First, the data protection problem in digital trade can be discussed within a trade agreement without further discussing harmonization of different legal agreements. In other words, trade participants do not need to lean on the discussion frame of harmonizing the general international law and trade law anymore. In general, a human rights issue has been considered as non-trade issue and thus it had been debated through the general exception clause of the GATT or GATS. However, persuading trade counterpart by using the provision of general exception is not an easy task

as discussed before. Data protection of digital trade succeeded in combining two different legal issues into one integral subject throughout recent legal developments.

Second, data protection regulations are advocating consumer rights of digital trade procedures. Considering that most of trade remedies concentrate on protecting *collective interests* of specific *industries*, data protection regulation has its distinctive aspect in that it deals with *individual consumer interests*. As representative trade remedy measures of the WTO, all safeguards measures, including anti-dumping duties and counter vailing duties can be imposed on the basis of collective interests of certain domestic industries. Agreement on Implementation of Article VI of the GATT 1994 ruling anti-dumping practices said that an investigation must be based on an evaluation containing specific approval rate expressed by its domestic producers. The approval rate should take up certain amount of total production of the like product.⁵⁹ Agreement on Subsidies and

⁵⁹ Article 5 (Initiation and Subsequent Investigation)

5.4 An investigation shall not be initiated pursuant to paragraph 1 unless the authorities have determined, on the basis of an examination of the degree of support for, or opposition to, the application expressed¹³ by domestic producers of the like product that the application has been made by or on behalf of the domestic industry. The application shall be considered to have been made "by or on behalf of the domestic industry" if it is supported by those domestic producers whose collective output constitutes more than 50 per cent of the total production of the like product produced by that portion of the domestic industry expressing either

Countervailing Measures also has a similar rule saying that countervailing duties can be imposed after an investigation on supporting degree of certain industry.⁶⁰ However, most of the international trade agreements on the personal information issue are clearly aware that the issue is related with individual consumer rights and reliabilities of companies using personal information. The TTIP emphasizes the importance of maintaining a dialogue among parties for consumer protection. The TPP has provisions on consumer protection saying that parties recognize the significance of adopting transparent and effective measures to protect consumers from fraudulent and deceptive commercial activities.

support for or opposition to the application. However, no investigation shall be initiated when domestic producers expressly supporting the application account for less than 25 per cent of total production of the like product produced by the domestic industry.

⁶⁰ Article 11 (Initiation and Subsequent Investigation)

11.4 An investigation shall not be initiated pursuant to paragraph 1 unless the authorities have determined, on the basis of an examination of the degree of support for, or opposition to, the application expressed³⁸ by domestic producers of the like product, that the application has been made by or on behalf of the domestic industry.³⁹ The application shall be considered to have been made "by or on behalf of the domestic industry" if it is supported by those domestic producers whose collective output constitutes more than 50 per cent of the total production of the like product produced by that portion of the domestic industry expressing either support for or opposition to the application. However, no investigation shall be initiated when domestic producers expressly supporting the application account for less than 25 per cent of total production of the like product produced by the domestic industry.

2. Limits of Existing Regulations

Despite legal developments under the WTO regime, several loopholes still exist in regulating recent data protection in trade procedures such as inconsistent application range of the GATS and ineffectiveness of relief measures of the DSU are few of those limitations embedded in the current WTO regulations. In other words, the “WTO agreements and most trade agreements do not contain languages that link governments’ obligations to protect, respect, and remedy violations of human rights to government’ obligations for trade.”⁶¹

Just as the judgement by the AB members of China-Publications and Audiovisual Products case, if digital contents without physical form were regulated under the GATS provisions, there would be a lot of digital service trades that cannot be applicable to the GATS rule. Different from the GATT which has negative method of ruling, the GATS is based on the positive method of regulation which only allows specifically stipulated services to be applied. Thus, the new forms of digital services that were not recognized at the time of legislation cannot be regulated according to the GATS. And thus, personal data protection problems aroused under the new types of trade

⁶¹ Susan Ariel Aaronson. 2016. *The Digital Trade Imbalance and Its Implications for Internet Governance*. CIGI. Chatham House. 21.

service procedure would not be protected under the current GATS regulation.

Moreover, even if certain types of trade service can be regulated under the GATS, whether remedy measures of the DSU can be an effective option for resolving data protection problems for each individual remain questionable. Since the dispute resolution measures of the DSU premises inter-governmental relationship, individual privacy concerns would be difficult to be resolved under the DSU mechanism. Because leaked information in the online area is hard to be retrieved completely according to the current WTO regulation, individual rights such as the right to be forgotten cannot be recognized. Even though there might be human right infringements over the course of the data flow between its member countries, human right protection is not a concern for the WTO as there is no legal obligation that could *bring members into conformity*.⁶²

However, the EU-US Privacy Shield Principle is an unprecedented

⁶² Article 19 (Panel and Appellate Body Recommendations)

1. Where a panel or the Appellate Body concludes that a measure is inconsistent with a covered agreement, it shall recommend that the Member concerned bring the measure into conformity with that agreement. In addition to its recommendations, the panel or Appellate Body may suggest ways in which the Member concerned could implement the recommendations.

2. In accordance with paragraph 2 of Article 3, in their findings and recommendations, the panel and Appellate Body cannot add to or diminish the rights and obligations provided in the covered agreements.

trade agreement in that it successfully brought the data protection issue up as human rights concern in the international trade legislation. Although other trade agreements such as the TiSA, several FTAs, TTIP and TPP all contain obligation for the data protection, the EU-US Privacy Shield Principle has the most concrete and progressive regulations. Unlike other trials depending on the existing system of the WTO as avoiding further specific rules, the Privacy Shield has its own independent and effective conflict resolution mechanism.

Firstly, the EU-US Privacy Shield Principles do not require individuals who claims privacy violations gather other claimants for filing a suit against the U.S. companies. Anyone can lodge complaints and get proper measures without any cost for arbitration, panel procedure, and ombudsperson supports.

In addition, the Privacy Shield has its own binding force to rectify or discontinue unjustifiable practices of companies. If a company persistently fails to comply, the company would no longer be listed on the Shield company list and obtain private information of the EU citizens. The article 11, dispute resolution and enforcement concerning the persistent failure, is as below:

ii. *“Persistent failure to comply arises where an organization that has self-certified to the Department refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution, or government body, or where such a body determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001). An organization’s withdrawal from a private-sector privacy self-regulatory program or independent dispute resolution mechanism does not relieve it of its obligation to comply with the Principles and would constitute a persistent failure to comply.”*

iii. *“The Department will remove an organization from the Privacy Shield List in response to any notification it receives of persistent failure to comply, whether it is received from the organization itself, from a privacy self-regulatory body or another independent dispute resolution body, or from a government body, but only after first providing 30 days’ notice and an opportunity to respond to the organization that has failed to comply. Accordingly, the Privacy Shield List maintained by the Department will make clear which organizations are assured and which organizations are no longer assured of Privacy Shield benefits.”*

The privacy violation under the Privacy Shield must be rectified within a specific period following the obligations unless the company is willing to forgo its right to receive personal information from the EU.

3. Harmonization of Data Protection Regulations in Trade Area

According to a research conducted by ITIF,⁶³ despite the regional efforts to tackle down unnecessary restrictions, many countries still maintain their own regulations blocking data flows at the national levels.⁶⁴ These disparities and protectionist approaches cause market participants to pay additional cost and deter maximization of market efficiency. Legal harmonization not only enhances market effectiveness but prevents forum shopping and assures predictability of participants. As an indefinite legal area which does not have unified multilateral frame to regulate the trade practice, the privacy protection calls for keen attention to its harmonization.

Harmonizing regulations on the issue would benefit both consumers of the EU and service providers in the U.S. in the long run. After the Snowden revelations that the U.S. information authority monitored phone calls and internet records of foreign citizens, one survey found that “56% of respondents felt hesitation to work with US-based cloud service

⁶³ Information Technology and Innovation Foundation (ITIF) is an “independent research and educational institute mainly dealing with the intersection of technological innovation and public policy.” <https://itif.org>.

⁶⁴ Niel Cory. 2017. “Cross-Border Data Flows”. Accessed January 7. 2018. <https://itif.org/databarriers>.

providers.”⁶⁵ Against this background, the U.S. firms faced the burden of protecting EU consumers’ privacy. However, satisfying various privacy protection standards is highly expensive for the U.S. companies and they might try to lobby its government for enhancing international unity over this issue by persuading the EU. Thought out these processes, the EU-US Privacy Shield Principles is expected to serve as a building block for unifying personal data protection standards under the international trade regime.

Although the EU and the U.S. reveal different perspectives on the specific methods to employ for regulation, the two trade giants who have set rules of international trade arena already made compromise through the EU-US Privacy Shield. It contains the most specific regulations on the data protection issue and can be a model agreement for other countries. The EU Ambassador to the U.S. said that the “negotiations provide an opportunity to develop regulatory coherence on privacy.”⁶⁶ Annegret Bendiek and Evita Schmieg also added that the “EU-US Privacy Shield will not solve the problem of legal uncertainty for firms operating on both sides of the Atlantic, nor will it set rules for data transfer outside the transatlantic market. But

⁶⁵ Susan Ariel Aaronson and Rob Maxim. 2013. *EU Data Protection Reform: Opportunities and Concerns*. 285.

⁶⁶ Delegation to the United States. Ambassador Joao Vale de Almeida on TTIP. 10 September 2013.

does at least open the door for future legal integration.”⁶⁷ Meanwhile, the EU-US Privacy Shield went into effect on 12 July 2016 and many US service providers have been preparing according to the change. The precedent experiences of the two trade giants would be a guide post for following years.

⁶⁷ Annegret Bendiek and Evita Schmieg. 2016. *European Union Data Protection and External Trade: Having the Best of Both Worlds*. 7.

V. Conclusion

Along with the increased volumes and impacts of digital trade, concerns over the protection of private data have been raised recently. However, different regulations among countries undermine consistency of data protection and hinder free flow of information. Misuse of personal data threatens human rights and causes additional cost in related industries. Although several countries are trying to narrow down the gap by introducing bilateral and preferential agreements among like-minded countries, most of those efforts are not enough to secure privacy protection and not effective in providing remedy measures for the individuals.

Legal experiences of the European Union would be worthy to examine in that the developments reflect unique characteristics of data protection issue which stands in the middle of human rights and international trade areas. In particular, the EU-US Privacy Shield Principles stipulate comparably more concrete and direct resolution procedures than other international trade agreements. Whereas the previous mechanisms only recognize collective interests of specific industry, the Privacy Shield Principles protect individuals as “consumer”.

Moreover, there are partially participating countries holding their own different regulations that do not correspond to the purpose of multilateral

trade regime in which all members should be treated equally. Even worse, non-parting countries would also find it much easier to circumvent when dealing with data transaction than traditional trade forms. Accordingly, expanding participation scope and enhancing conformity of regulation on the issue would be critical. On the way to harmonization, the EU-US Privacy Shield Principle can suggest a guide post and the international trade partners can further develop integrated regulation for balancing between the data free flow and personal data protection.

Bibliography

English References

Alexander Dix. 2013. *EU Data Protection Reform: Opportunities and Concerns*.

Leibniz Information Centre for Economics.

Annegret Bendiek and Evita Schmieg. 2016. *European Union Data Protection and External Trade*. German Institute for International and Security Affairs.

Daniel T. Shedd, Brandon J. Murrill and Jane M. Smith. 2012. *Dispute Settlement in the World Trade Organization: An Overview*. Congressional Research Service.

European Commission. 2016. *Guide to the EU-US Privacy Shield*.

European Commission. 2016. *Trade in Service Agreement Fact Sheet*.

Jong Duk Kim. 2013. *Trade in Services Agreement (TISA) and Services Liberalization in Korea*. KIEP.

Mary E. Footer. 1997. *The Role of Consensus in GATT/WTO Decision-making*. Northwestern Journal of International Law and Business.

Martin A. Weiss and Kristin Archick. 2016. *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*. Congressional Research Service.

Niel Cory. 2017. *Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?* ITIF.

Samuel Gibbs. 2015. *What is 'Safe Harbour' and Why Did the EUCJ just Declare it Invalid?* The Guardian.

Susan Ariel Aaronson. 2016. *The Digital Trade Imbalance and Its Implications for Internet Governance*. CIGI. Chatham House.

Susan Ariel Asonson and M. Townes. 2012. *Can Trade Policy Set Information Free: Trade Agreements, Internet Governance and Internet Freedom*. Policy Brief.

UNCTAD. 2016. *Data Protection Regulations and International Data Flows: Implications for Trade and Development*.

UNCTAD. 2016. *Investment and Digital Trade*. World Investment Report 2016.

Vivian Reding. Data Protection Reform: Restoring Trust and Building the Digital Single Market. Speech Delivered at the 4th Annual European Data Protection &

Privacy Conference Brussels. 17 September 2013.

Korean References

KOTRA. 2017. EU 디지털 단일시장 전략의 평가와 시사점.

KIEP. 2015. 국제 디지털 상거래의 주요 쟁점과 한국의 대응방안.

Sang-Yook Cha. 2017. *A Study on Recent Legislations related with Personal Information Protection in EU and Its Implications.*

Official Documents

Case C-362/14. Maximillian Schrems v. Digital Rights Ireland Ltd.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Official Journal of the European Union L 119/1 2016/679

Report of the Appellate Body. The U.S.-Measures Affecting the Cross-Border Supply of Gambling and Betting Service.

Report of the Appellate Body. China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products.

Online Resources

<http://boykoborissov.bg>

<http://www.export.gov>

<http://www.guengl.eu>

<http://www.worldtradelaw.net>

<http://www.wto.org>

<https://itif.org>

<https://rm.coe.int>

<https://www.coe.int/en/web/data-protection>

<https://www.computing.co.uk>

<https://www.privacyshield.gov>

국문 초록

디지털 무역의 개인정보보호와 통상협정 : 유럽연합법 발전을 중심으로

디지털 기술의 발전과 더불어 일상의 많은 상품과 서비스의 거래 역시 디지털화된 형태로 이뤄지고 있다. 이러한 교환 과정에는 민감한 개인정보의 이전이 필연적으로 동반되고 있고 자칫 악용 될 수 있어 정보보호에 대한 불안감이 높아지고 있다. 하지만, 전통적 형태의 무역이 주를 이루던 때의 모습을 담고 있는 세계무역기구(WTO) 체제 하의 규정을 비롯해 대부분의 국제 통상 협정에서는 이 과정에서 발생할 수 있는 개인정보보호 문제를 효과적으로 다루고 있지 못한 실정이다.

이에 본 연구는 오랫동안 개인정보보호 문제를 인권보호의 문제로 인식해 법리를 발전시켜온 유럽연합(EU)의 노력을 살펴보았다. 특히, 이러한 노력이 EU가 역외국가와 맺은 국제통상법 상에 어떻게 반영되어 권리 보호와 구제 장치를 마련해 두었는지 WTO 규정과 양·다자간 자유무역협정(FTA) 규정들과 비교해보았다.

흥미로웠던 점은 이러한 규정들이 개인정보보호 문제를 인권과 소비자 보호의 관점에서 접근하여 그간 통상법의 관심에서 벗어나 있던 인권 문제를 자연스레 통상법 내로 가져와 다루고 있는 것이었다. 다만, 갈등해결과 관련해서 대부분의 FTA들은 명확한 지침을 두지 않거나 국가간 갈등해결과 규정예의 합치에 중점을 둔 WTO 협정 내의 분쟁해결양해를 차용하고 있어 개인의 권리구제 측면에서는 한계가 있는 것으로 보인다.

이와 달리, 2015년 Safe Harbor 협정의 무효 판정 이듬해 EU와

미국 간에 새롭게 맺어진 Privacy Shield 협정은 EU 소비자들의 개인정보를 역외로 이전하여 가는 미국 기업들의 개인 정보보호 의무에 대해 가장 상세한 규정을 두고 있었다. 기존의 통상협정들이 국가간 갈등의 문제로서 소의 이익 또한 자국산업의 집단이익에서 찾던 데 반해, 해당 규정은 미국 기업에 대응한 EU 시민 개인의 권리 보호와 구제를 위한 적극적이고 실질적인 규정을 포함하고 있다.

아직까지는 데이터 이전과 개인정보보호와 관련하여 다자체제 하의 통일된 규정이 없는 한편 각국은 각기 다른 수준의 규제를 취하고 있어 기업의 추가적인 거래 비용과 소비자의 권리보호를 위협하는 등 무역 효율성을 저하시키고 있다. EU와 미국은 규범정립을 주도하고 있는 국제무대의 주요 행위자로서 양측이 이미 합의를 하여 둔 Privacy Shield 원칙들은 향후 국제 규범의 일원화를 위한 중요한 지침이 될 수 있을 것이다.

주제어: 디지털 무역, 개인정보 보호, EU-US Privacy Shield, 권리 구제, 규범 조화

학번: 2013-22071